Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of enabling software development for an integrated circuit, ~~the integrated circuit being configured to run a boot program that prevents unverified software from subsequently being loaded onto, or run by, the integrated circuit by use of a digital signature to verify software loaded onto, or run by, the integrated circuit,~~ the method including the ~~step~~ steps of:

running a boot program on the integrated circuit which verifies programs before said programs can be loaded onto, or run by, the integrated circuit by verifying whether said programs are signed with a boot key;

verifying, with the boot program, a developmental boot program signed with the boot key which verifies developmental programs before said developmental programs can be loaded onto, or run by, the integrated circuit by verifying whether the integrated circuit has a predetermined integrated circuit identifier; and

loading ~~an intermediate~~the verified developmental boot program onto the integrated circuit~~, the intermediate~~ and running the loaded developmental boot program ~~being customised for a particular one or more of a plurality of potential integrated circuits that, when run on the integrated circuit, enables~~ thereby enabling loading or running of ~~unverified code~~said developmental programs on ~~only the particular one or more~~ the integrated ~~circuits without use of a digital signature~~circuit if the integrated circuit has the integrated circuit identifier.

2-4. (Canceled)

5. (Currently Amended) An integrated circuit configured to:

run a boot program that ~~prevents unverified software from subsequently being~~ verifies programs before said programs can be loaded onto, or run by, the integrated circuit by ~~use of a digital signature to verify software being loaded onto, or run by, the integrated circuit~~verifying whether said programs are signed with a boot key;

verify, with the boot program, a developmental boot program signed with the boot key which verifies developmental programs before said developmental programs can be

loaded onto, or run by, the integrated circuit by verifying whether the integrated circuit has a predetermined integrated circuit identifier; and

load the verified developmental boot program and run ~~an intermediate~~ the loaded developmental booth program ~~customised for a particular one or more of a plurality of potential integrated circuits that, when run on the integrated circuit, enables~~thereby enabling loading or running of ~~unverified code~~said developmental programs on ~~only the particular one or more~~the integrated ~~circuits without use of a digital signature~~circuit if the integrated circuit has the integrated circuit identifier.

6. (Original) An integrated circuit according to claim 5, programmed with program code configured to:

receive software data and a digital signature of the software data

generate a first digest from the software data; and

compare the first digest against a second digest obtained via the digital signature that accompanied the received software data;

wherein the program is considered valid when the first and second digests match.

7. (Original) An integrated circuit according to claim 6, wherein one or both of the digests were generated using a SHA1 function.

8. (Original) An integrated circuit according to claim 6, wherein the boot program contains a plurality of keys, and one of the keys is selected for use in generating the first digest, the key being selected in accordance with a selection criterion.

9. (Original) An integrated circuit according to claim 8, wherein the selection criterion is time-based, a particular one of the keys being selected depending on the time the selection is made.

10. (Original) An integrated circuit according to claim 8, wherein the selection criteria relates to a physical arrangement or configuration of the integrated circuit.

11. (Original) An integrated circuit according to claim 10, wherein the physical arrangement or configuration includes one or more of the following:

one or more pads wired to a reference voltage or to ground;

one or more fuses, one or more of which has been blown; or

the contents of non-volatile memory.

12. (Original) An integrated circuit according to claim 5, programmed with program code configured to:

receive encrypted software data,

decrypt the software data; and

validate the software data;

wherein the decrypted software is executed only when the validation is successful.

13. (Original) An integrated circuit according to claim 12, wherein the encryption function is RSA.

14. (Original) An integrated circuit according to claim 12, wherein the boot program contains a plurality of keys, and one of the keys is selected for use in decrypting the software data, the key being selected in accordance with a selection criterion.

15. (Original) An integrated circuit according to claim 14, wherein the selection criterion is time-based, a particular one of the keys being selected depending on the time the selection is made.

16. (Original) An integrated circuit according to claim 14, wherein the selection criteria relates to a physical arrangement or configuration of the integrated circuit.

17. (Original) An integrated circuit according to claim 16, wherein the physical arrangement or configuration includes one or more of the following:

one or more pads wired to a reference voltage or to ground;

one or more fuses, one or more of which has been blown; or

the contents of non-volatile memory.